CLAIMS

1. A method for authenticating digital data in a system for writing digital data entered from an input device to a memory and transferring the digital data written in the memory to a receiving device, said method comprising the steps of:

when writing digital data from the input device to the memory and transferring the digital data from the memory to the receiving device, authenticating devices between the input device and the memory and between the memory and the receiving device respectively; and

when writing digital data to the memory, in the case of implementing on the digital data an electronic signature by a one-way hash function and also reading from the memory and transferring the digital data, decrypting the implemented electronic signature so as to transfer the digital data after ensuring that it has not been changed since it was recorded.

2. The method of claim 1 comprising the step of:

mixing data for authenticating devices into the digital data to be written from said input device to said memory and the digital data to be transferred from said memory to said receiving device.

3. The method of claim 1 comprising the step of:

implementing by a central processing unit built into said memory authentication between said input device and said receiving device and authentication to the digital data in said memory and decryption of said implemented authentication.

4. The method of claim 1 comprising the step of:

only if authentication between said input device and said memory and between said memory and said receiving device is successful, performing the writing of digital data from said input device to said memory and the transfer of digital data from said memory to said receiving device; and if the authentication is not successful, performing ordinary writing and transfer of digital data.

5. The method of claim 1 wherein:

between said input device and said memory, said system having a specific mutual encryption function Hdc and an internal key Kdc used for authenticating both of them; said memory having a hash function Hcf and an internal key Kcf used for an electronic signature in said memory; and between said memory and said input device, said system having a specific mutual encryption function Hpc and its key Kpc used for authenticating both of them.

6. The method of claim 5 wherein said functions Hdc, Hcf and Hpc and their keys Kdc, and Kcf are stored in a read-only memory of said memory device.

7. The method of claim 6 wherein said key Kpc is encrypted and stored in NAND record space.

8. The method of claim 1 wherein authentication from said input device to said memory is performed by using a public key system.

9. The method of claim 1 wherein said memory is a flash memory and stores said electronic signature on digital data by said hash function into a redundant area not to be calculated by an ECC of each page in an memory area.